Universidade de Brasília Faculdade UnB Gama

Criptografia e Segurança de Redes
Trabalho 2

Alunos: Matrículas:
João Paulo Nunes Soares 15/0038267
Josué Nascimento da Silva 15/0038933

- INSTRUÇÕES DE USO
  - **Exercício 1**
    - Para compilar o arquivo execute na pasta do arquivo: **gcc aes.c -o main** .
    - Para executar o programa execute: **./main**
    - Após executar escolher as opções desejadas, inserindo a chave e o texto desejado
  - **Exercício 2**
    - Para resolução do exercício 2, foi escolhido a implementação do CTR utilizando o DES como cifrador.
    - Para compilar o arquivo execute na pasta do arquivo: **gcc ctr.c -o main** .
    - Para executar o programa execute: **./main**
    - Após executar,escolha a opção desejada e insira os valores na ordem solicitada e a mensagem decifrada ou cifrada será mostrada.

- LIMITAÇÕES CONHECIDAS
  - **Exercício 1**
    - Devem ser inseridos na mensagem e na chave somente caracteres hexadecimais maiusculos (0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F);
    - O Programa trabalha apenas com mensagens e chaves de 128 bits
    - Deve-se respeitar os tamanho de chave e mensagem, caso contrario o programa apresentará erros de funcionamento
    - O Programa cifra apenas um único bloco de 128 bits , caso queira-se cifrar um novo bloco de 128, deve-se selecionar novamente a opção de criptografar
  - **Exercício 2**
    - Devem ser inseridos na mensagem e na chave somente caracteres hexadecimais minúsculos (0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f);
    - Caso o tamanho da mensagem seja inserido errado(número que não é múltiplo de 64), o programa apresentará erro em seu funcionamento.

- ✔ Caso a quantidade de caracteres inseridos como mensagem não respeite o tamanho em bits inserido anteriormente, o programa apresentará erro em seu funcionamento.

- DIVISÃO DO TRABALHO
  - ✔ Ambos os alunos realizaram a atividade, onde a maior parte foi realizada no modelo de pareamento.